

# From Incident to Resolution: Managing Cyber Claims Successfully

A Marsh webinar  
November 30, 2023

# Our speakers



**John Scordo**

Managing Director  
Cyber Claims Advocacy Leader  
Marsh Specialty



**Sherri Davidoff**

CEO  
LMG Security



**Patrick Cannon**

Head of Cyber Claims  
Claims Solutions  
Marsh Specialty

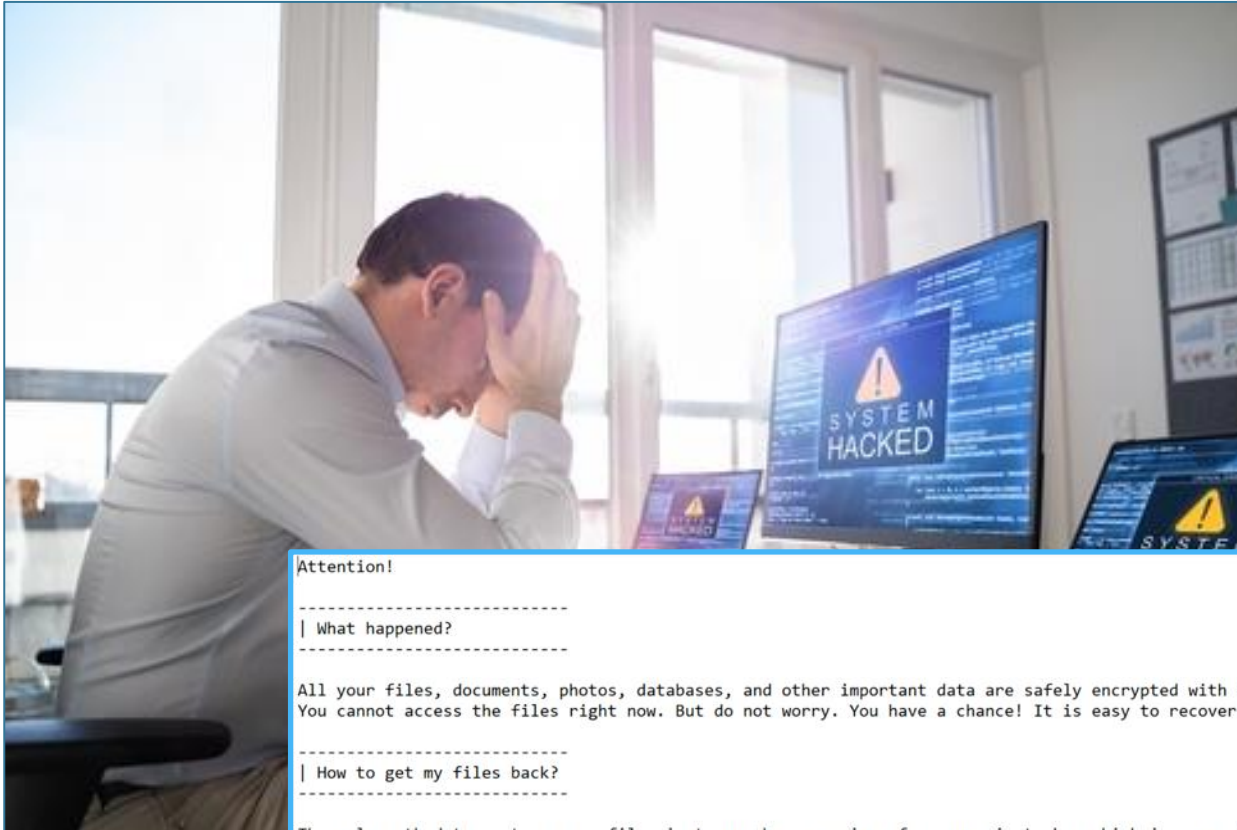
1. Overview of Claims
2. Case Study: A Ransomware Attack in Action
3. Cyber Incident Management
4. Widespread Events and Global Impacts
5. Role of Cyber Insurance
6. Common Coverage Problems

# Agenda

# Types of Cyber Events

ACTORS	CYBER EVENTS	BUSINESS EVENTS	LOSSES	INSURANCE
<ul style="list-style-type: none"> <li>• External Actor – Malicious</li> <li>• External Actor – Accident</li> <li>• Internal Actor – Malicious</li> <li>• Internal Actor – Accident</li> <li>• Internal Actor – Intentional</li> <li>• Third Party Partner – IT Vendor</li> <li>• Third Party Partner – Other Vendor</li> <li>• Third Party Partner – Customer</li> <li>• None</li> <li>• Unknown</li> <li>• Other</li> </ul>	<ul style="list-style-type: none"> <li>• Unauthorized Access To Network</li> <li>• Lost, Stolen Equipment</li> <li>• System Failure, Interruption, Degradation</li> <li>• Fraud, Trick, Social Engineering, Impersonation</li> <li>• Data Collection, Sharing</li> <li>• System Overwhelmed, DDOS</li> <li>• Error In Entering Data</li> <li>• Software Misconfiguring</li> </ul>	<ul style="list-style-type: none"> <li>• Data Breach – Accessed</li> <li>• Data Breach – Exfiltrated</li> <li>• Extortion</li> <li>• Fund Transfer Fraud</li> <li>• Data Encrypted, Deleted or Altered</li> <li>• Business Interruption</li> <li>• Crypto Jacking</li> <li>• Privacy Law Violation</li> </ul>	<ul style="list-style-type: none"> <li>• Breach Response Legal Costs</li> <li>• Breach Response Forensic Costs</li> <li>• Breach Response Notification Costs</li> <li>• Breach Response Remediation Costs</li> <li>• Extortion Payment and Costs</li> <li>• Data Restoration Costs</li> <li>• Business Interruption Revenue or Profit Loss</li> <li>• Extra Expense Costs</li> <li>• Regulatory Loss</li> <li>• Claim, Litigation Loss</li> <li>• Defense Cost Loss</li> <li>• Equipment, Software Replaced</li> <li>• Loss of Funds</li> <li>• Liability for Loss of Funds</li> <li>• Loss of Expected Account Receivable</li> </ul>	<ul style="list-style-type: none"> <li>• Cyber</li> <li>• Tech Error and Omission</li> <li>• Kidnapping and Ransom</li> <li>• Crime</li> <li>• Property</li> <li>• Other</li> </ul>

# Case Study: A Business is Held Hostage



- Computers offline
- POS are all down
- Data encrypted
- Ransom notes

Attention!

-----  
What happened?

All your files, documents, photos, databases, and other important data are safely encrypted with reliable algorithms. You cannot access the files right now. But do not worry. You have a chance! It is easy to recover in a few steps.

-----  
How to get my files back?

The only method to restore your files is to purchase a unique for you private key which is securely stored on our servers. To contact us and purchase the key you have to visit our website in a hidden TOR network.

There are general 2 ways to reach us:

1) [Recommended] Using hidden TOR network.

a) Download a special TOR browser: <https://www.torproject.org/>  
b) Install the TOR Browser.  
c) Open the TOR Browser.



# Ransom Note

Attention!

-----  
What happened?

All your files, documents, photos, databases, and other important data are safely encrypted with reliable algorithms. You cannot access the files right now. But do not worry. You have a chance! It is easy to recover in a few steps.

-----  
How to get my files back?

The only method to restore your files is to purchase a unique for you private key which is securely stored on our servers. To contact us and purchase the key you have to visit our website in a hidden TOR network.

There are general 2 ways to reach us:

- 1) [Recommended] Using hidden TOR network.
  - a) Download a special TOR browser: <https://www.torproject.org/>
  - b) Install the TOR Browser.
  - c) Open the TOR Browser.



# Voicemail from the Criminals





# Data Exposure is a Trend

Professional PR/media engagement

Paid staff & consultants



HOME NEWS ABOUT CONTACT US

Auction platform

Data theft & exposure



Welcome to the Karakurt hacking team website. You can browse and download the files that were leaked. Read our news. Learn more about us and on how we operate.

team ad the ews. we

**March aucti**

23 FEB 2022, 16:20:28

We've been pret months and had outside auction :

Our lair is into 3 stages\rrooms\levels call it what you want. The deeper you get the worse is your situation.

---

## PRE-RELEASE

KARAKURTS DON'T BITE FIRST NEITHER DO WE. AT THIS POINT WE ARE JUST WEAVING THE WEB BY GATHERING AND SORTING YOUR COMPANIES INFORMATION. WE ARE DOING IT VERY GENTLY AND OBSERVING THE VICTIM FROM THE DISTANCE. YOU ARE STILL SAFE.

---

## RELEASING

WHEN THE VICTIM TRAPS INTO KARAKURTS WEB THERE IS NO WAY BACK. WELCOME TO OUR PLACE. STICKY WEB, ISN'T IT? IN OTHER WORDS YOUR INFORMATION IS BEING UPLOADED INTO OUR AUCTION PLATFORM. ONCE UPLOADING IS FINISHED - YOU ARE IN TROUBLE.

---

## RELEASED

Karakurts poison is very toxic and dangerous. Doit waste your time. What would you do? Of course you will have to take an antidote. In your situation it means that you still have a chance to survive. But it will cost as double. All you need is to accept our terms and conditions without any sort of bargain.

DESIGNED BY SANDRA BULLOCK





RANSOM  
DEMAND:  
\$1,200,000



# Dead in the Water

- Client files - gone
- Shared folders – gone
- Payroll details – gone
- HR data – gone
  - & more
- Clients depended on them for daily bookkeeping etc.



# Cyber incident management

## Why is incident management important?



Cyber incidents are going to happen



Effective incident management lessens the impact



**95%**

Percentage of cybersecurity incidents occur due to human error.

Source: World Economic Forum Global Risks Report 2022



**USD 2.66 million**

Average cost savings associated with an incident response (IR) team and regularly tested IR plan.

Source: IBM Cost of a Data Breach Report 2022



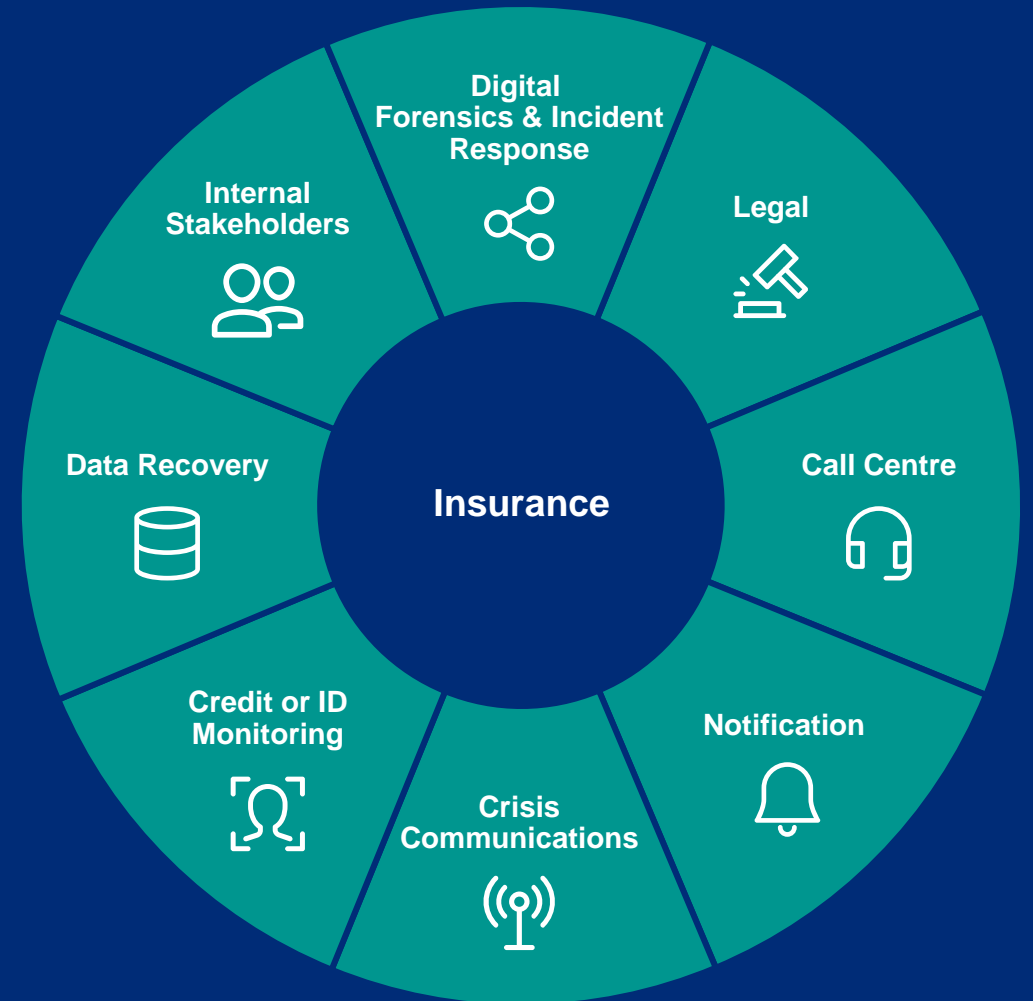
**2.46%**

Average share performance loss following a cyber incident, but significant variance between companies that respond well (7.9% increase) versus those that respond badly (12% loss).

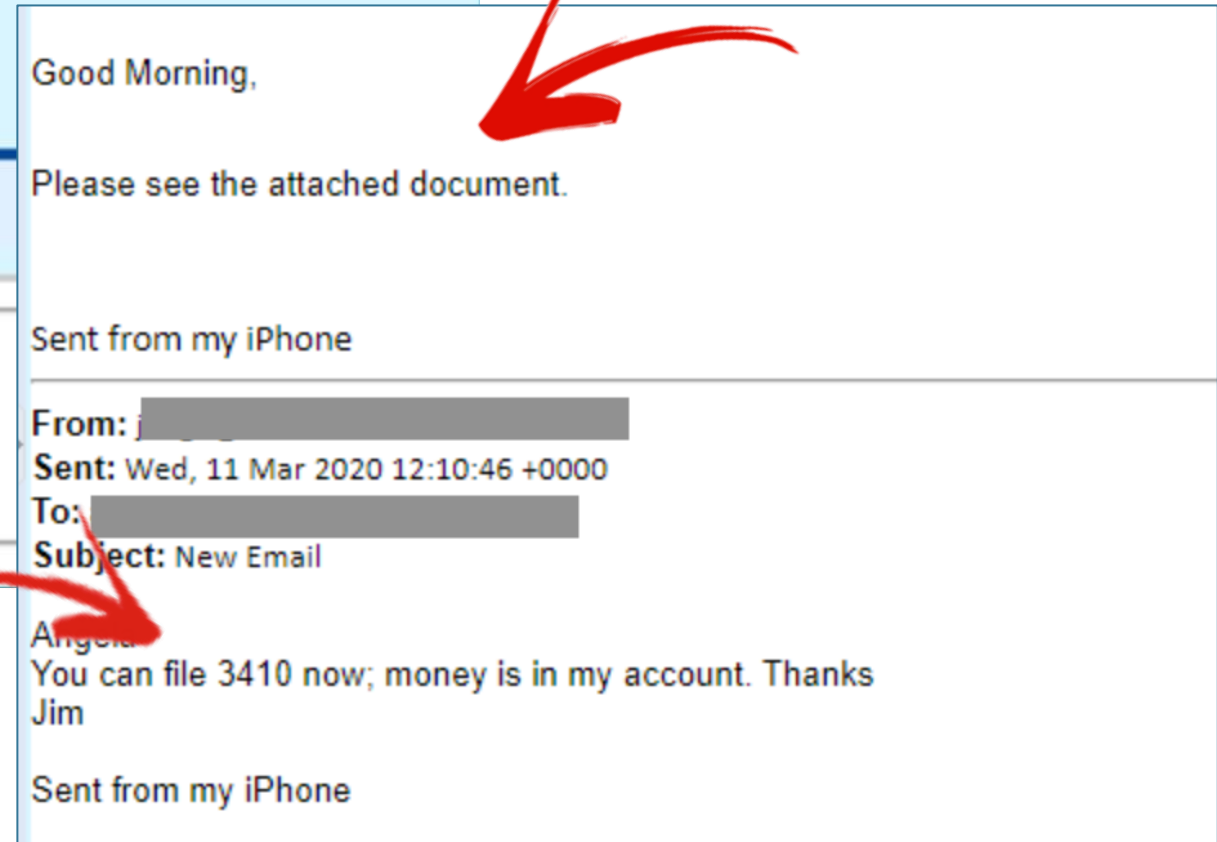
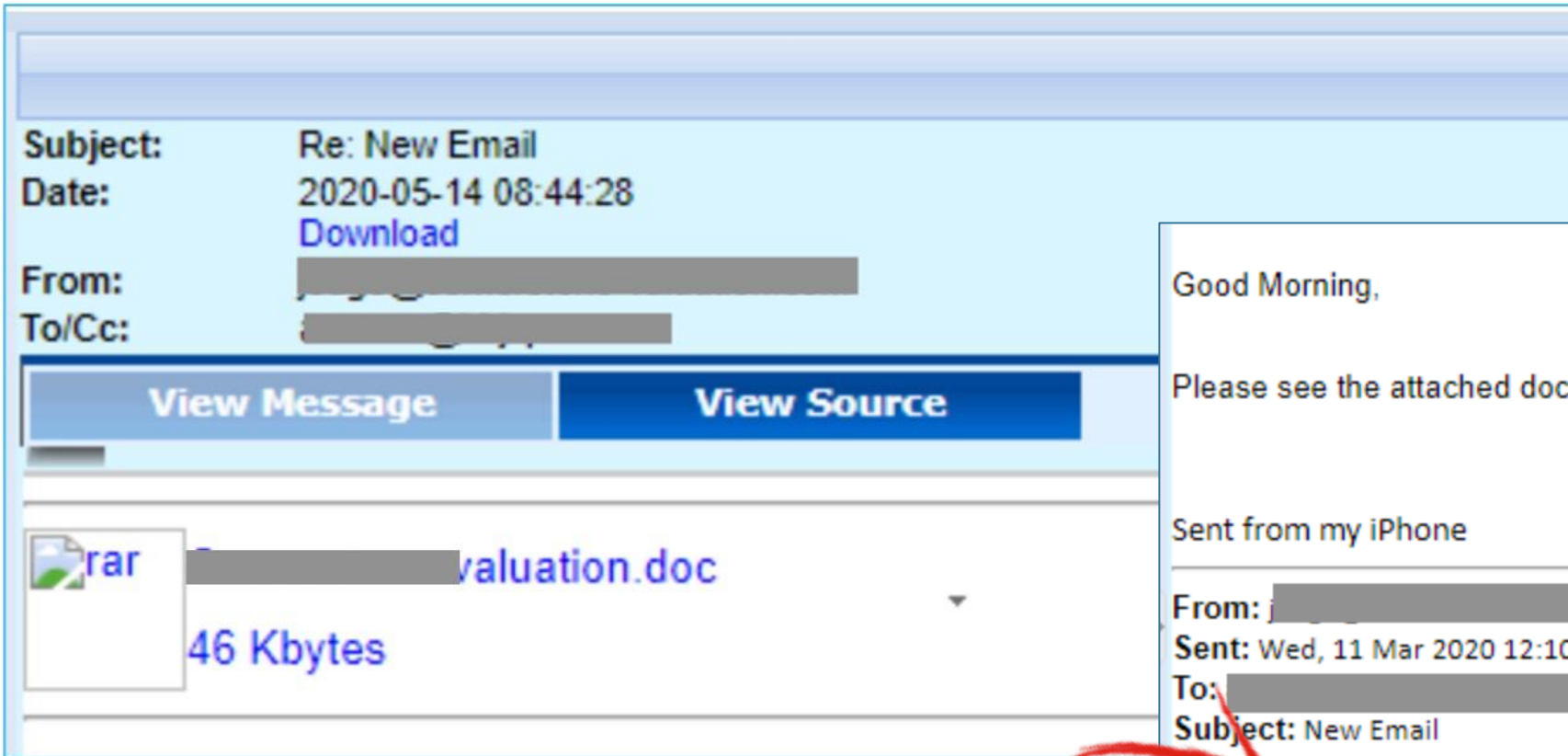
Source: Marsh – Survive or Thrive: How Crisis Impact Company Value

# Critical steps to take

- Successful resolution of cyber incidents requires expert coordination of multiple vendors and work streams.
- Immediate engagement of legal counsel is critical.
- Vendors assist with investigation/recovery and help ensure that all legal and regulatory obligations are fulfilled.
- A typical cyber insurance policy has a vendor 'panel' built in and is usually accessible via a 24/7 hotline.



# “Email Reply Chain” Phishing Attack



And then, they lurked...



# Smash-and-Grab

- Criminals remotely logged on to had
- Stole passwords
  - Username/pwd of admin
- Took full control of network
- Mass data transfer to mega.co.nz
  - ~500 GB
- Deployed ransomware



# The Criminals Were Watching Communications

Good morning,

I think you still cannot understand what situation your company is in now. But you are not the first and you are not the last who think that nothing terrible has happened. But believe in our experience that you are greatly mistaken.

**We know that you are trying to restore the network from backups. But the biggest losses for you will be from the publication of data that will be sued by both your employees and your clients.**

It is unlikely that someone wants to provide their personal data to a company that cannot save them.

We also saw the report that [redacted] provided you. It contains many errors. If you want to receive a full report on penetration, you need to contact us.

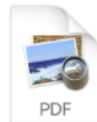
We also want to note that We did not specifically encrypt all computers on the network. We have fixed on some of them and will repeat the attack at any time. Once again, we advise you to weigh all your future losses and

**We also saw the report that [redacted] provided you. It contains many errors. If you want to receive a full report or penetration, you need to contact us.**

P.S. We are sending you some files with private info as proofs. And You have 1 day left to contact us. Read our rules here <https://mazenews.top/>



100183 GA  
K1.pdf



100183 MD  
K1.pdf



# The Criminals Promise to Delete The Stolen Data



Ok, confirm. Please upload one DECRYPT-FILES.txt from each machine and we will send you archive with decryptors.

05:29:00 PM | Today

The data holder will now proceed to wiping of data and making full file tree, it can take up to few days, as it takes some time.

05:29:20 PM | Today





## Good

- Backups are available
- Network secured
- Threat hunting complete







## Bad

- Maze has the data
- Ransom of \$565,000
- Notifications are still needed







# Cyber coverage parts

## First party coverages

		DESCRIPTION	COVERED COSTS
<b>First Party Cover</b> 1 <sup>st</sup> Party Insurance coverage: direct loss and out of pocket expense incurred by insured			
	<b>Business Income/ Extra Expense</b>	Interruption or suspension of computer systems due to a network security breach. Coverage may be added to include system failure and can extend to contingent businesses.	<ul style="list-style-type: none"> <li>• Loss of Income</li> <li>• Costs in excess of normal operating expenses required to restore systems</li> <li>• Dependent business interruption</li> <li>• Forensic expenses</li> </ul>
	<b>Data Asset Protection</b>	Costs to restore, recreate, or recollect your data and other intangible assets that are corrupted or destroyed.	<ul style="list-style-type: none"> <li>• Restoration of corrupted data</li> <li>• Vendor costs to recreate lost data</li> </ul>
	<b>Event Management / Breach Response</b>	Costs resulting from a network security or privacy breach.	<ul style="list-style-type: none"> <li>• Forensics</li> <li>• Notification</li> <li>• Credit Monitoring</li> <li>• Call Center</li> <li>• Public Relations</li> </ul>
	<b>Cyber Extortion</b>	Network or data compromised if ransom not paid.	<ul style="list-style-type: none"> <li>• Forensics</li> <li>• Investigation</li> <li>• Negotiations and payments of ransoms demanded</li> </ul>

# Cyber coverage parts

## Third party coverages

	DESCRIPTION	COVERED COSTS
<b>Third Party Cover</b> 3rd Party insurance coverage: defense and liability incurred due to alleged harm caused to others by the insured.		
	<b>Privacy Liability</b> Failure to prevent unauthorized access, disclosure or collection, or failure of others to whom you have entrusted such information, for not properly notifying of a privacy breach.	<ul style="list-style-type: none"><li>• Liability and defense</li><li>• Bank lawsuits</li><li>• Consumer lawsuits</li></ul>
	<b>Network Security Liability</b> Failure of system security to prevent or mitigate a computer attack. Failure of system security includes failure of written policies and procedures addressing technology use.	<ul style="list-style-type: none"><li>• Liability and defense</li></ul>
	<b>Privacy Regulatory Defense Costs &amp; PCI Fines &amp; Penalties</b> Privacy breach and related fines or penalties assessed by Regulators.	<ul style="list-style-type: none"><li>• Liability and defense</li><li>• Investigation by a regulator</li><li>• Prep costs to testify before regulators</li><li>• PCI / PHI fines and penalties</li></ul>
	<b>Media Liability</b> Defense and liability for, including but not limited to, libel, slander, product disparagement, misappropriation of name or likeness, plagiarism, copyright infringement, etc.	<ul style="list-style-type: none"><li>• Liability and defense</li></ul>

# Getting your claim paid quickly

Use panel vendors!

Average time from notification to confirmation of cover or first payment:



Panel vendors used

**2.1** months



Non-panel vendors used

**12.7** months



# Trend: Global Widespread Events

- What is a widespread event?
- Zero-day vulns
- Cloud
- Examples:
  - Microsoft Exchange
  - Blackbaud
  - Log4j
  - MOVEit
  - Now: Cisco
  - & Many more!





## Number of Cisco Devices Hacked via Unpatched Vulnerability Increases to 40,000

The number of Cisco devices hacked via the CVE-2023-20198 zero-day has reached 40,000, including many in the US.

*Image source: Screenshot of Shodan output taken in LMG's lab*


# Software Exploits are Trending on the Dark Web

0day.today - Biggest Exploit Database In the World. Select your language: 





## 0DAY.today?

Things you should know about 0day.today:

- We use one main domain: <http://0day.today>
- Most of the materials is **completely FREE**
- If you want to **purchase the exploit / get V.I.P. access** or pay for any other service, you need to buy or earn  **GOLD**

We accept currencies: [contact]



-::GOLD	-::AUTHOR
 0.097	0day Today Team
 0.116	0day Today Team
 0.147	0day Today Team
 0.058	crash.poc
 0.155	0day Today Team
 0.193	muxbear
 0.116	macos0day
 0.039	jiehu
 0.001	!m0Nk3y_
 0.004	_null_



## Number of known victims of the MOVEit attack so far:

2380 organizations

66.2 - 71.1 m individuals



Last updated November 8, 2023

MOVEit® Transfer

## Secure Managed File Transfer Software for the Enterprise

In a world built on distributed work and collaboration, securing sensitive files is essential. Simplify, automate, and take control of MFT with Progress MOVEit, the leading secure managed file transfer application. Ensure management and control over your business-critical file transfers by consolidating them all on one system.

## Moveit Transfer flaw leads to wave of data breach disclosures

Organizations that have confirmed a data breach tied to the critical Moveit flaw disclosed in May include the government of Nova Scotia, the BBC and HR software firm Zellis.



# Happy Memorial Day!

- May 27<sup>th</sup>, 2023: TA505 (Clap) begins actively exploiting MOVEit servers
- Sensitive files stolen from exploitable MOVEit hosts
  - An undisclosed number of victims were impacted
- Both on-premise and SaaS versions
- Clap told victims to contact them or their data would be published





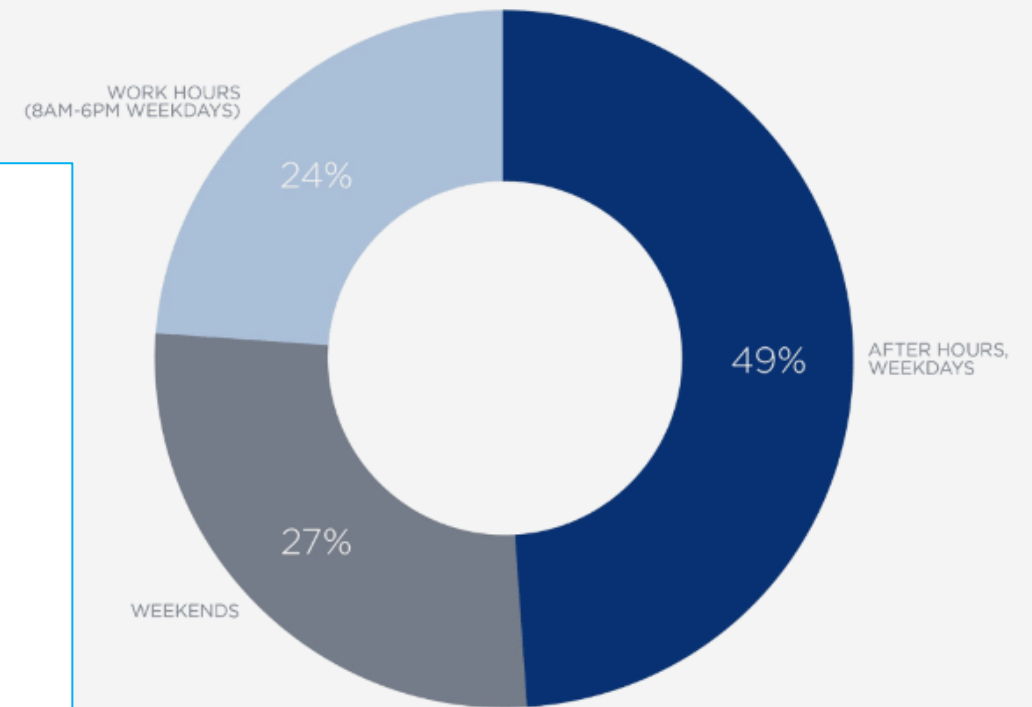
# This Timing Isn't Unusual

- Memorial Day weekend
  - Coincidence? Unlikely
  - “Forensics Friday” @LMG
- Who’s on call for your organization?
- Who is monitoring threat intelligence?

In **76%** of cases, ransomware was executed outside work hours



OBSERVED RANSOMWARE DEPLOYMENT  
WORK HOURS VS. AFTER HOURS



FIREEYE™



CLOP IS ONE OF TOP ORGANIZATION OFFER PENETRATION TESTING SERVICE AFTER THE FACT.

THIS IS ANNOUNCEMENT TO EDUCATE COMPANIES WHO USE PROGRESS MOVEIT PRODUCT THAT CHANCE IS THAT WE DOWNLOAD ALOT OF YOUR DATA AS PART OF EXCEPTIONAL EXPLOIT. WE ARE THE ONLY ONE WHO PERFORM SUCH ATTACK AND RELAX BECAUSE YOUR DATA IS SAFE.

*STEP 1 - IF YOU HAD MOVEIT SOFTWARE CONTINUE TO STEP 2 ELSE LEAVE.*

*STEP 2 - EMAIL OUR TEAM UNLOCK@RSV-BOX.COM OR UNLOCK@SUPPORT-MULT.COM*

*STEP 3 - OUR TEAM WILL EMAIL YOU WITH DEDICATED CHAT URL OVER TOR*

**WHAT WARRANTY?** OUR TEAM HAS BEEN AROUND FOR MANY YEARS. WE HAVE NOT EVEN ONE TIME NOT DO AS WE PROMISE. WHEN WE SAY DATA IS DELETE IT IS CAUSE WE SHOW VIDEO PROOF. WE HAVE NO USE FOR FEW MEASLE DOLLARS TO DECEIVE YOU.

CALL TODAY BEFORE YOUR COMPANY NAME IS PUBLISH HERE.



# Hackers Target File Sharing Services!

- High-value assets
- Cloud & on-prem
- 2021 – Accellion File Transfer Appliance (FTA)
  - 0-day vuln
  - Dozens of orgs announced breaches
- 2023 – GoAnywhere
  - 0-day vuln
  - ~135 victims were hacked (Feb 2023)
- Russian-affiliated gang (“Clop”)

## Clop ransomware claims it breached 130 orgs using GoAnywhere zero-day

By [Sergiu Gatlan](#)

February 10, 2023 03:15 PM 0

## Months after the Accellion breach, more victims emerge

The Accellion breach occurred last December, but more victims have come to light in recent weeks as investigations, notifications and disclosures stretch on through the summer.



# More Data = Higher Damages When it Leaks



Per-record cost of a data breach

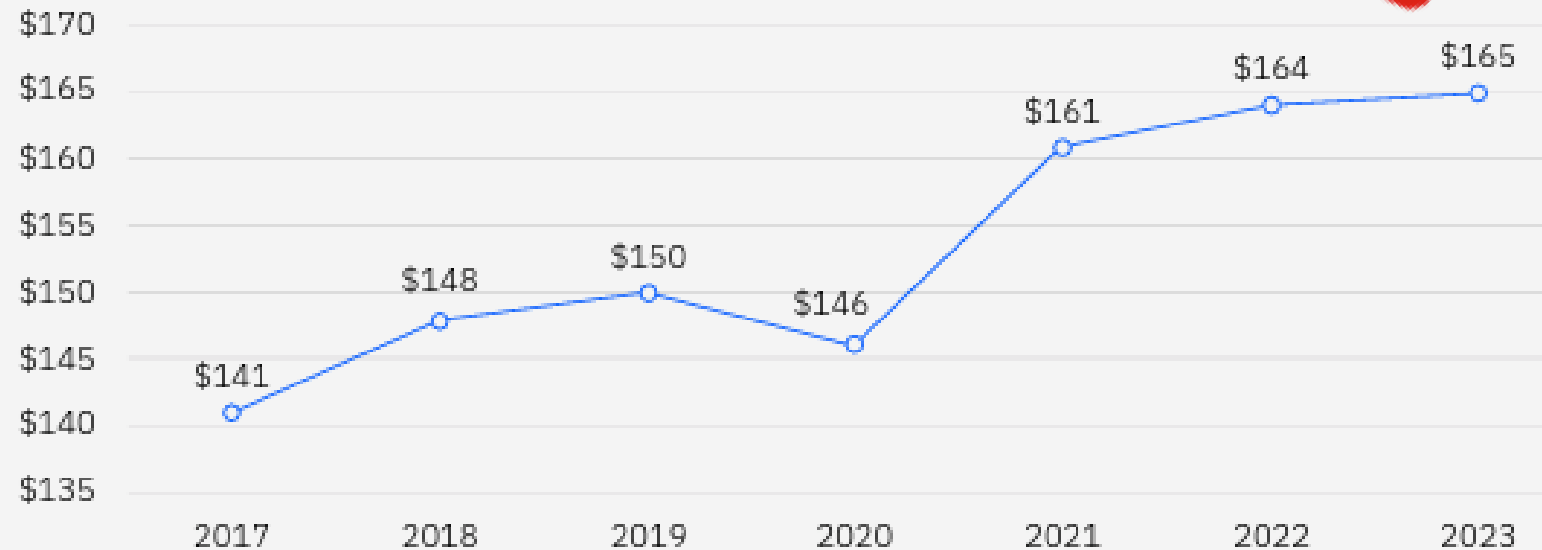


Figure 2. Measured in USD



# Reduce Your Data

- Automatic retention/deletion times
- Limit data provided to suppliers
- Supplier deletion SLAs

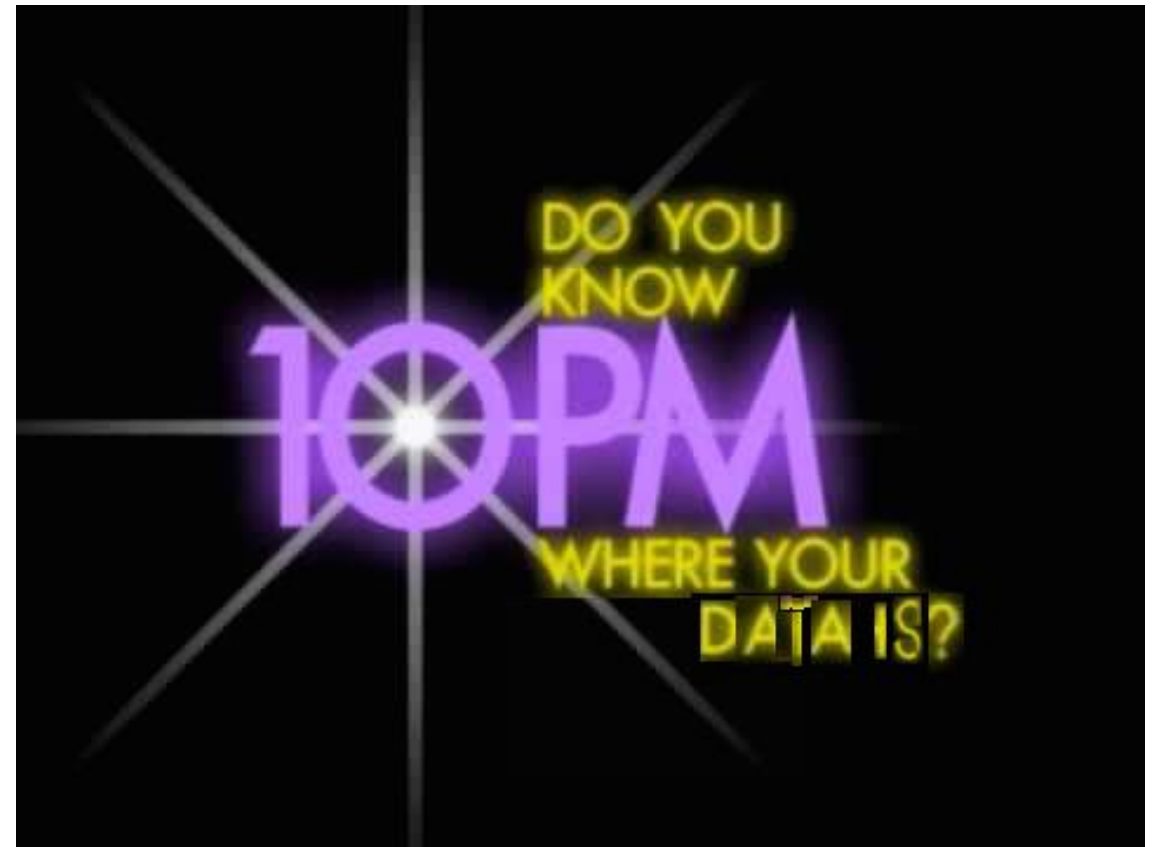
The Cheapest Way to Reduce  
Your Risk!





# Maintain an Accurate Data & Asset Inventory

- Make sure you have an up-to-date inventory of assets
- Identify sensitive data
- Local Network & Cloud/SaaS
- Automated Tools
- Include 3<sup>rd</sup> party suppliers!



# Coverage or reimbursement issues

- Carefully select panel counsel and other vendors
- Review attorney rates and vendor scope of work
- Consider other insurance
- Evaluate upgrades or betterment
- Review in-house labor
- Factor in computer forensic/data recovery
- Assess third-party claims and credits
- Explore theft of funds
- Monitor business interruption
- Consider extra expenses





# Update & Test Your Incident Response Plans

- Plan for zero-day software exploits
- Practice, practice, practice!
- Educate IT staff & responders
- Clarify roles & responsibilities
- Test processes, communications, etc.
- Integrate your insurance into your IR documentation



USD 2.66 million

Average cost savings associated with an incident response (IR) team and regularly tested IR plan

IBM, “Cost of a Data Breach 2023”





# To learn more



**John Scordo**

Managing Director  
Cyber Claims Advocacy Leader  
Marsh Specialty  
john.scordo@marsh.com



**Sherri Davidoff**

CEO  
LMG Security  
info@LMGsecurity.com



**Patrick Cannon**

Head of Cyber Claims  
Claims Solutions  
Marsh Specialty  
patrick.cannon@marsh.com

